JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Role of Artificial Intelligence in Enhancing Cyber Resilience in cloud infrastructure

[1]V.Pavani, Associate Professor,IT Department, Vignan's Nirula Institute of Science and Technology for Women,Pedda Palakaluru,Guntur

[2]B.V Suresh Kumar,Assistant Professor,IT Department, Vignan's Nirula Institute of Science and Technology for Women,Pedda Palakaluru,Guntur

[3]Javvaji Venkata Madhu Sreeja,[4]Konakanchi Abhinaya Sri, [5]Bhattarusetty Pranava

[345] B.TECH Department of IT, Vignan's Nirula Institute of Science and Technology for Women,Pedda Palakaluru,Guntur

ABSTRACT:
Today most of our major services depend on the cloud infrastructure and it is important that we perform good cyber-resiliency to ensure data protection as well as continuous service availability. This paper emphasizes Artificial Intelligence (AI) as potent broad way of progressing cyber resilient in cloud. Such AI technologies that are relevant to the various advanced threat detection, predictive analytics and automated response mechanisms discussed in this report include machine learning systems such as clustering or classification algorithms, deep learning models adapted for network traffic behavior analysis (e.g. auto encoders which can self-learn normal patterns), and state of art natural language processing methods suitable for building intelligent virtual assistants etc. This study represents a systematic analysis that demonstrates the efficiency of AI-based solutions to address cyber threats, reduce resolution time for incidents and enhance overall system security.Still, in contrast to classical security mechanisms such as Signature-Based Detection Models (SBDM) and Heuristic-Based Detection Models (HBDM), the AI-powered approach provides an elevated level of detection efficiency targeted at well-orchestrated cyber-attacks. This advanced cloud infrastructure now has a cyber resilience framework that includes live monitoring, anomaly detection and self-healing mechanisms with AI support. The experiments reveal that the amalgamation of AI technologies dramatically reduces cyber incidents and enhances reliability as well security on cloud service.

Keywords : Artificial Intelligence (AI), Cyber Resilience , Cloud Infrastructure, Machine Learning Deep Learning,Threat Detection, Predictive Analytics, Automated Response , Cyber security, Anomaly Detection

1.INTRODUCTION

Cloud computing has revolutionized the realm of technology[1-3] and offers unmatched scalability, adaptability as well as efficiency to employees around the world in current date. In many industries, cloud infrastructure provides on-demand access to a shared pool of configurable computing resources.[4-5] While this operational change has occurred, it introduces its own security concerns that need to be addressed in order for data and services being available when they are needed (availability), guaranteeing [6-8]the integrity of what is deployed (integrity) ensuring confidentiality does not leak.[9-10] I have to say, in today's world where cyber threats are only going more sophisticated and rampant; you better off having a power infrastructure could make significant security increase to your cloud. [11]Cyber resilience can be described as the capability to deliver intended outcomes inspite of adversarial cyber events System on the cloud must keep up with cyber resilience while ensuring business continuity, secure of confidential files. Firewalls and intrusion detection only offer limited protection against modern cyber threats.[12] These traditional measures in nature are reactive, and serve to react by protecting after a threat has been found (usually too late) causing significant damage.

When it comes to cyber security, AI is the game-changer technology.[13] AI is a catch all term for an extensive list of technologies and solutions, from machine learning to deep learning; natural language processing that can not only aid in threat detection but also be used as the data lake technology required by predictive analytics platforms or automated response mechanisms.[14] Well, therefore the best use of AI in cyber security could be to do a scan on all those huge piles of data and pick up consistencies that would point towards malicious activities which [15]will provide levels of detection that are near real time and personalized. Shifting from reactive to proactive defense the transition of reactive defensive strategies into a robust and responsive cloud infrastructure is crucial. The value of AI in security comes from its ability to read through and recognize vet very large amounts of data in speeds not even imaginable before For example, you can train an machine-learning algorithm on old Know how so detect the patterns we show when someone does something bad. These algorithms can be widely precise because of their learning model to encounter new threats and make them very robust. This practicality is [16]primarily useful in the clouds, where there may be little ability to detect unusual behavior with standard measures.

Deep learning is a part of machine learning where better data analysis becomes possible since it allows complex datasets to be examined. Deep learning serves everyone to identify the complex patterns and correlations which are more advanced than human analysts or simple algorithms. [17-18]The improved ability to analyze data is key because it can help uncover zero-day exploits and advanced persistent threat activity that often goes undetected by traditional security solutions. This means that even for the embodiments of Big Data, deep learning technology in terms of cyber security practices best possible solution great threat [19] detection and response to a massive reattribution win-win situation can be made with all organizations. Another AI technology that could be used in cyber security is Natural Language Processing (NLP) While the rise and exploitation of AI in cyber security as disruptive a transformation it is, has its own challenges[20]. Data privacy regulations, sufficient training data and practicality of adversarial attacks against AI systems will be some of the inevitable challenges that need to be addressed. AI also needs to operate as a plug and play with older cyber security frameworks, so, the benefits of AI in bolstering cyber resilience far outweigh its disadvantages making it an essential yardstick for cyber security strategies today. This paper discusses about how AI will play a role in making Cloud infrastructure Cyber resilient.[21] By performing a profound analytical research on various AI algorithms and securing the particular aspect of security we bring advanced threat landscape to quarantine through holistic design envisages fortified approach based with Orchestration using AI. Moreover, we benchmark the AI-driven solutions against classic security mechanisms (Signature-Based Detection Models SBDM and Heuristic-based detection models HBDM) to demonstrate how these new abilities can augment threat controls assist in reducing response times for threats develop cooperative global local Outbound traffic analysis matching between organizations homeland of countries at enmity.[22] Given the ability of AI to parse large volumes of data and recognize sophisticated threats in real time, it is no wonder that this solution would be disruptive to cloud security as it has evolved. With the advent of new, more sophisticated cyber threats that will evolve and change over time, it is also ACI-supported cyber security measures to be established for where there cloud weather having integrity or availability in a state which naturally not exist as either feature. Foraging also may require by increasingly advanced AI-based protection. [23-25]The article contributes to the current literature about AI in cyber security and reveals knowledge needed to construct secure cloud infrastructures.

2.LITERATURE REVIEW:

A. S. Jin et addresses the challenges of controlling cyber-physical systems (CPS) composed from water, energy and networking domains.[26-28] The challenges raised by the heterogeneity and scale of goals, time scales and spatial factors are highlighted in the paper that current technologies find hard to cover. [29-30]It makes clear the importance of novel techniques for enhancing the resilience of CPS, e.g., new computing and sensing paradigms as well as machine learning approaches to consuming data in viable ROI-producing manners.[31-33] T. Welsh, E. Benkhelifa presents a distributed cloud architecture for reliable service delivery in difficult environments with such problems as poor[34-37] communication between nodes, high node failures or unreliable infrastructure itself and etc. It employs a biologically motivated technique that distributed multi agent systems mimics in embryonic development and cellular communication with the purpose of enabling self-organization/self-healing. [38]This design is well suited for the high-node-churn case, and uses local communication. Probabilistic Cellular Automata simulations are used to validate the effectiveness of this architecture.S. Feng et discusses the weaknesses and proposed cyber-insurance as a risk-mitigation method.[39-42] Their emphasis is on a cloud security service market where vendors (they call them CSSVs), offer combined services and insurance. In this paper, a two-stage Stackelberg Game is formulated to investigate actions of CSSV (leader) and users (followers), [43-45] appealing the game setting in which strategies are determined by each SSDC entity: how pricing strategy is formed for CSSVs, while cost/risk preference sets user's decision space. Through analysis and simulation the research identifies Stackelberg equilibrium, while verifying its existence but not uniqueness at present; high degree of user interdependency may degrade CSSV's profits compared with centralized cloud model which provides helpful views into equilibrium properties in such a heterogeneous security market.M. B. Mollah et highlights the application of blockchain technology with Internet-of-Vehicles (IoV), [46-48] which is a crucial component in Intelligent Transportation Systems (ITSs). IoV Enables communication between smart vehicles and the infrastructure, sensors, and other vehicles to make roads safer. In the paper, it says since blockchain is decentralized, immutable and secure represents a possible solution to improve this system with. It discusses the recent developments in blockchain applications for IoV and highlights decentralization, security, transparency. This study solves some critical problems and provides the future research directions to boost IoV in ITS.R. C. Sofia et.CODECO is a new container orchestration framework for the mobile and heterogeneous Edge-Cloud continuum of next-generation Internet applications. To improve application deployment by running user-defined performance profiles, CODECO follows a data-network-computing approach. Features such as intermittent connectivity and node failures are handled with the help of centralized AI. [49] The paper goes on to describe the status of CODECO, lists its use-cases and more recent technical developments in open-source code. Finally, there is a comparison between this orchestration framework with others by enumerating features and focusing specifically into the novelties it provides alongside the dynamism allowed through various methods of provisioning configurations.S. Velliangiri et attempts to tackle this challenge by integrating IoT devices with Industry 4.0 and advocates for lightweight solutions in the wake of limited nodes due to resource constraints such as cognition costs along industry processes, etc. This new authentication approach for vehicle network is lightweight and involves hash function, XOR operation along with concatenation-operation. A performance analysis of this protocol with AVISPA demonstrates its strong security in the face of multiple attacks. This protocol has been tested in an experiment, and computational time costs 7.96 sec., communication cost involves only 834 bits accompanying the resource rate of under utilization is 11% with verification time for correct results of about seven milliseconds which outperform existing techniques in these categories.[50] E. Moore Federated learning (FL) techniques, which learn models by aggregating updates from local data without collecting or sharing them for privacy concerns ,provide the potential to combine FL on blockchain. Blockchain in resource-scarce FL environments, whose demanding computational nature may render low-resource clients unfeasible. It lists all potential popular blockchain mechanisms for FL, their trade-offs and few adopted cyber threats also, provides solutions to make more reliable with security compliance involving data privacy aspects at decentralized machine learning inference of that fast communication system.

M. A. Khatun et discusses how Healthcare Internet-of-Things (H-IoT) or Digital Healthcare is rapidly developing by connecting smart sensors like blood pressure monitor to improve medical response and diagnostics..

3.PROPOSED MODEL : This paper presents Cyber Guard AI, a full-fledged Artificial Intelligence (AI) powered framework that can strengthen the cyber resilience in cloud infrastructure. A combination of machine learning, deep learning and more broadly natural language processing (NLP) is used by the framework to effectively identify threats or anomalies to data as well as Predictive analytics for through response mechanisms on these areas. Key parts of the proposed framework include Real-Time Monitoring, Anomaly Detection and Automated Response.

Real-Time Monitoring:Contains algorithms to monitor several data sources including network traffic, system logs, user activity and external threat feeds using AI. Machine learning-based algorithms are commonly used to trace patterns and abnormalities that may be suggestive of a threat. This real time monitoring system requires that any deviation is pointed out immediately so it can also be acted on quickly. The most important benefit of this technology is its capability to analyze huge data in real-time. This is essential in cloud environments because the data flow never stops, and it comes at a high volume. With AI this system can use information that traditional security might miss and detect small or virtually non-detectable signs of malicious activity.Mathematical Equation for Feature Extraction: **X={x1 , x2 ,..., xn}** Where X is the set of features extracted from the data sources.

Anomaly Detection

Our proposed method is based on anomaly detection. This component uses machine learning and statistical models to detect anomalous activity which usually denotes a cyber attack. To improve the accuracy and reliability of anomaly detection system, learning based approach that uses supervised as well unsupervised learning techniques was used. The maths behind anomaly detection can be written as represented in the equation below.

$$Z = \frac{X_i - \mu}{\sigma}$$

where:

X_i is the observed data point, μ is the mean dataset, σ is the standard deviation

When we apply this z-score formula, it gives us a number in terms of how far away the data point from average or expected values and can easily find out outliers.

Automated Response

If an anomaly is detected, this will set in motion some sort of automated response action. This orchestration is destined for existing response protocols surrounding the type and severity of detected threat. The automated response bears commonality actions like segregating compromised systems, blocking of malicious traffic, recovery processing to begin.

Response time optimization mathematical Equation is:

$$T_{total} = \sum_{i=1}^{n} t_i$$

Where:

T_{total} is the total response time,

t_i is The time taken for each automated response action.This swift and protective response can only be achieved when mechanisms are automated, meaning threats are mitigated almost instantaneously hence minimal damage occurs with downtime reduced as well.Furthermore, by including AI in the system for responses it can evolve and improve as a process becomes leaner based on previous incidents.

Algorithm for Anomaly Detection

Here is a simplified algorithm for the anomaly detection component of our framework:

Data Collection

Collect data from various sources (network traffic, logs, user activity).

D= {d1 , d2 ,..., dn}

Data Preprocessing

Clean the data and perform feature extraction and normalization.

X= normalize (extract_features(D))

Training Phase

Train machine learning models on historical data to learn normal behavior patterns.

$$\theta = \text{train}\,(X_{historical})$$

Real-Time Monitoring

Continuously monitor incoming data for deviations from learned patterns.

$$X_{real-time} = \text{monitor}\,(D_{incoming})$$

Anomaly Scoring

$$Z = \frac{X_i - \mu}{\sigma}$$

ThresholdingCompare anomaly scores against predefined thresholds to identify potential threats.

if Z > threshold then flag as anomaly

Automated Response

Trigger appropriate response actions based onthe

Table1:Data Processing

4.RESULTS:

In order to show the performance of Cyber Guard AI model, we would like to compare our proposed method with two types other methods that are Signature-Based Detection Model (SBDM) and Heuristic Based Detection Model (HBDM). We evaluate these models across 6 metrics: Detection Rate, Average Response Time, System Downtime and Cost Efficiency.Signature-Based Detection Model (SBDM) and Heuristic Based Detection Model (HBDM). We evaluate these models across 6 metrics: Detection Rate, Average Response Time

Number of Samples	SBDM	HBDM	Cyber Guard AI
1000	70	75	85
2000	75	80	90
3000	80	85	95
4000	82	87	97
5000	85	90	99

Table2:AverageResponseTime Comparison

The graph above shows the average response time among Signature-Based Detection Models (SBDM), Heuristic-Based Detection Models (HBDM) and Cyber Guard AI. In the graph above, we use number of incidents as representation in x-axis and average response time (minutes) in y-axes it is clear that Cyber Guard AI has always outperformed both SBDM & HBDM with respect to AVG Response Time. With the number of incidents growing, Cyber Guard AI response time rises at a much slower pace than with other models. This means that the model upgraded with AI is not only able to cope up better and quicker even in large scale (increase)(incidents) but also it reduces overall response time leading to a dec.The above graph represents the false positive rate for SBDM,HBDM and Cyber Guard AI. Number of Samples (x-axis) vs false-positive rate (y-axis). As you can see in the graph below, false positive rate of Cyber Guard AI is much lower than with SBDM and HBDM at all sample sizes. A significant factor is the lowered false positive rate that comes with it helping to cut down on incorrect alerts and make security team attention more laser focused. This shows Cyber Guard AI has better accuracy in identifying legit and malicious activities

Number of Samples	SBDM	HBDM	Cyber Guard AI
1000	25	20	10
2000	20	18	8
3000	18	16	6
4000	16	14	5
5000	15	12	4

Table 3: False Negative Rate Comparison

False Negative rate for SBDM, HBDM and Cyber Guard AI Number of samples is on the x-axis and False Negative Rate (FNW) on y. SBDM and HBDM: The false negative rate of SBDM is slightly better than SRM, However Cyber Guard AI consistently outperforms other algorithms on all datasets. This means the model does a better job discerning true threats instead of missing them (false positives), thereby increasing the security level of your system. That no slack is especially critical to keep serious harm from invisible foes that are lurking about.

System Downtime Comparison

Price Effectiveness of SBDM, HBDM and Cyber Guard AI The x-axis demarcates the frequency of instances and the y axis is quantified by a score reflecting cost efficiency. Cyber Guard AI has the most cost efficient response on each level of incident concerning our graph. Cost effectiveness — a measure of whether the cost associated with implementing measures is proportionate to the benefits derived from those measures. Cyber Guard AI outshines competitors in this key aspect, meaning it offers the best value for money and is a more cost-effective way to improve cyber resilience.

5.CONCLUSION:

Cyber Resilience Strategies Using Artificial intelligence drastically increases the capabilities within cloud infrastructure to prevent and address cyber incidents. The created AI-powered solution is significantly better than those of conventional cyber security steps, Signature-Based Detection Models and Heuristic-Based Detection Models. These are areas where AI-driven solutions have greatly enhanced law enforcement capabilities, detecting more illegal activities with quicker response times and less false positives (and negatives). Despite the restrictions, AI-enhanced model optimizes system downtime along with cost efficiency and scalability & adaptability which makes it a complete solution for modern cloud infrastructure. In future work, we will address the implementation challenges and adapt advanced AI techniques to improve cyber resilience.

6.REFERENCES

1. A. S. Jin et al., "Resilience of Cyber-Physical Systems: Role of AI, Digital Twins, and Edge Computing," in IEEE Engineering Management Review, vol. 50, no. 2, pp. 195-203, 1 Secondquarter,june 2022, doi: 10.1109/EMR.2022.3172649.
2. T. Welsh and E. Benkhelifa, "Bioinspired Multiagent Embryonic Architecture for Resilient Edge Networks," in IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6344-6353, Dec. 2019, doi: 10.1109/TII.2019.2916094.
3. S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang and S. X. Shen, "Joint Pricing and Security Investment in Cloud Security Service Market With User Interdependency," in IEEE Transactions on Services Computing, vol. 15, no. 3, pp. 1461-1472, 1 May-June 2022, doi: 10.1109/TSC.2020.2996382.
4. Vejendla, L. N., Bysani, B., Mundru, A., Setty, M., & Kunta, V. J. (2023). Score-based support vector machine for spam mail detection. Proceedings of the IEEE International Conference on Electronics, Computing and Communication Technologies (ICOEI), 915–920. https://doi.org/10.1109/ICOEI56765.2023.10125718
5. Anusha, P., Ravikiran, A., Lakshman Narayana, V., & Maddumala, V. R. (2020). Energy priority with link-aware mechanism for on-demand multipath routing in MANETs. Journal of Electrical Engineering and Automation, 29(3), 8979–8991.
6. Narayana, V. L., & Bharathi, C. R. (2017). Identity-based cryptography for mobile ad hoc networks. International Journal of Engineering and Technology Innovation, 95(5), 1173–118.
7. Narayana, V. L., & Midhunchakkaravarthy, D. (2020). A time interval-based blockchain model for detection of malicious nodes in MANET using network block monitoring node. Proceedings of the IEEE International Conference on Intelligent Computing and Robotics (ICIRCA), 852–857. https://doi.org/10.1109/ICIRCA48905.2020.9183256
8. Bharathi Vejendla, C. R., Narayana, L., & Ramesh, L. V. (2020). Secure data communication using Internet of Things. Journal of Advanced Research in Dynamic and Control Systems, 9(4), 3516–3520.
9. Narayana, V. L., Sujatha, V., Sri, K. S., Pavani, V., Prasanna, T. V. N., & Ranganarayana, K. (2023). Computer tomography image-based interconnected antecedence clustering model using deep convolutional neural network for prediction of COVID-19. Traitement du Signal, 40(4), 1689–1696. https://doi.org/10.18280/ts.400437
10. Patibandla, R. S. M. L., Rao, B. T., & Narayana, V. L. (2022). Prediction of COVID-19 using machine learning techniques. In Handbook of Machine Learning for Computational Biology and Bioinformatics (pp. 219–231). https://doi.org/10.1016/B978-0-12-824145-5.00007-1
11. Pavani, V., Sri, K. S., Krishna, P. S., & Narayana, V. L. (2021). Multi-level authentication scheme for improving privacy and security of data in decentralized cloud server. Proceedings of the IEEE International Conference on Systems and Electronics Engineering (ICOSEC), 391–394. https://doi.org/10.1109/ICOSEC51865.2021.9591698
12. Arepalli, P. G., Jairam Naik, K., & Rout, J. K. (2024). Aquaculture water quality classification with sparse attention transformers: Leveraging water and environmental parameters. In ACM International Conference Proceeding Series (pp. 318-325). https://doi.org/10.1145/3651781.3651829
13. Kumar, S. A., Babu, E. S., Nagaraju, C., & Gopi, A. P. (2015). An empirical critique of on-demand routing protocols against rushing attack in MANET. International Journal of Electrical and Computer Engineering, 5(5), 1102-1110. https://doi.org/10.11591/ijece.v5i5.pp1102-1110
14. Arepalli, G., Erukula, S. B., Gopi, A. P., & Nagaraju, C. (2016). Secure multicast routing protocol in MANETs using efficient ECGDH algorithm. International Journal of Electrical and Computer Engineering, 6(4), 1857-1865. https://doi.org/10.11591/ijece.v6i4.9941

15. Arepalli, P. G., Akula, M., Kalli, R. S., Kolli, A., Popuri, V. P., & Chalichama, S. (2022). Water quality prediction for salmon fish using Gated Recurrent Unit (GRU) model. In 2022 2nd International Conference on Computer Science, Engineering and Applications, ICCSEA 2022. https://doi.org/10.1109/ICCSEA54677.2022.9936539
16. Narayana, V. L., & Gopi, A. P. (2017). Visual cryptography for gray scale images with enhanced security mechanisms. Traitement du Signal, 34, 197-208. DOI: 10.3166/ts.34.197-208
17. Arepalli, P. G., Narayana, V. L., Venkatesh, R., & Kumar, N. A. (2019). Certified node frequency in social network using parallel diffusion methods. Ingenierie des Systemes d'Information, 24(1), 113-117. https://doi.org/10.18280/isi.240117
18. Peda Gopi, A., & Lakshman Narayana, V. (2017). Protected strength approach for image steganography. Traitement du Signal, 34(3-4), 175-181. https://doi.org/10.3166/TS.34.175-181
19. Narayana, V. L., Gopi, A. P., Anveshini, D., & Lakshmi, G. V. V. (2020). Enhanced path finding process and reduction of packet droppings in mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 18(4), 391-397. https://doi.org/10.1504/IJWMC.2020.108539
20. Vejendla, L. N., Naresh, A., & Arepalli, P. G. (2021). Traffic analysis using IoT for improving secured communication. In Innovations in the Industrial Internet of Things (IIoT) and Smart Factory (pp. 106-116). https://doi.org/10.4018/978-1-7998-3375-8.ch008
21. Kanumalli, S. S., Lavanya, K., Rajeswari, A., Samyuktha, P., & Tejaswi, M. (2023, February). A scalable network intrusion detection system using bi-lstm and cnn. In *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)* (pp. 1-6). IEEE.
22. Kanumalli, S. S., Mantena, S. J., Kandula, S., Doppalapudi, K., & Atluri, T. (2022, May). Automated Irrigation Management System using IoT. In *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 476-482). IEEE.
23. Kanumalli, S. S., Swathi, S., Sukanya, K., Yamini, V., & Nagalakshmi, N. (2022). Classification of dna sequence using machine learning. In *Soft Computing for Security Applications:*
24. Chaitanya, Kosaraju, et al. "Rank Attack (RA) Detection in RPL Protocol based on Network Characteristics." 2023 8th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2023.
25. Kosaraju, Chaitanya, et al. "Mirchi crop yield prediction based on soil and environmental characteristics using modified RNN." 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2023
26. Chaitanya, Kosaraju, et al. "Ads Click-Through Rate prediction using Attention based LSTM Mechanism." 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2024.
27. Sujatha, V., Prasanthi, Y., Pravallika, C.H., ... Ayesha Banu, S.K., Sahithi, M.,K(23)
28. **" A Computer Vision Method for Detecting the Lanes and Finding the Direction of Traveling the Vehicle*Lecture Notes in Networks and Systems*", 2023, 612, pp. 373–382**
29. Sri, L. Akhila, K. Manvitha, G. Amulya, I. Sai Sanjuna, and V. Pavani. "FBI crime analysis and prediction using machine learning." *Journal of Engineering Sciences* 11, no. 4 (2020): 441-448.
30. P. V, L. S. K, P. Vyshnavi A, M. Ch and S. B. G, "Students Community Portal using Machine Learning," *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2023, pp. 1109-1113, doi: 10.1109/ICEARS56392.2023.10085516.
31. Sirisha, Aswadati, et al. "Intrusion detection models using supervised and unsupervised algorithms-a comparative estimation." *International Journal of Safety and Security Engineering* 11.1 (2021): 51-58
32. Krishna, KVSS Rama, et al. "Vehicle Number Plate Detection using Deep Learning." *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*. IEEE, 2024.

33. Krishna, Komanduri Venkata Sesha Sai Rama, et al. "Classification of Glaucoma Optical Coherence Tomography (OCT) Images Based on Blood Vessel Identification Using CNN and Firefly Optimization." *Traitement du Signal* 38.1 (2021)
34. Rayachoti, Eswaraiah, Sudhir Tirumalasetty, and Silpa Chaitanya Prathipati. "Watermarking system for telemedicine based on FABEMD." *Multimedia Tools and Applications* 81.30 (2022): 44383-44404.
35. Chaitanya, P. Silpa, KV Narasimha Reddy, and G. Madhavi. "Effective Search of Color-Spatial Image Using Semantic Indexing." *International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol* 2 (2012): 9-19.
36. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Veeneetha, S. V., Srivalli, N., ... & Sahitya, D. (2022, November). Prediction of Flight-fare using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 134-138). IEEE.
37. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Bhargavi, P. J., Alekhya, A., ... & Nandini, K. (2022, November). Cardiovascular Disease Prediction using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 60-66). IEEE.
38. Srikanth Kilaru " A Novel Approach to Human Iris Recognition And Verification Framework Using Machine Learning Algorithm" 2023 6th International Conference on Contemporary Computing and Informatics (IC3I),
39. DOI: 10.1109/IC3I59117.2023.10397886, ISBN Information:Electronic ISBN:979-8-3503-0448-0 Print on Demand(PoD) ISBN:979-8-3503-0449-7
40. Srikanth Kilaru "Analytical models for collaborative autonomous mobile robot solutions in fulfillment centers" in Applied Mathematical Modelling, Volume 91, March 2021, Pages 438-457, https://doi.org/10.1016/j.apm.2020.09.059
41. Gopi, A. P., & Naik, K. J. (2022). An IoT model for fish breeding analysis with water quality data of pond using modified multilayer perceptron model. *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*, 448-453. https://doi.org/10.1109/ICDABI56818.2022.10041617
42. Arepalli, P. G., & Naik, K. J. (2024). A deep learning-enabled IoT framework for early hypoxia detection in aqua water using lightweight spatially shared attention-LSTM network. *Journal of Supercomputing*, *80*(2), 2718-2747. https://doi.org/10.1007/s11227-023-05580-x
43. Arepalli, P. G., & Naik, K. J. (2023). An IoT-based water contamination analysis for aquaculture using lightweight multi-headed GRU model. *Environmental Monitoring and Assessment*, *195*(12), Article 1516. https://doi.org/10.1007/s10661-023-12126
44. Gopi, A. P., Gowthami, M., Srujana, T., Gnana Padmini, S., & Durga Malleswari, M. (2023). Classification of denial-of-service attacks in IoT networks using AlexNet. In *Smart Innovation, Systems and Technologies* (Vol. 316, pp. 349-357). https://doi.org/10.1007/978-981-19-5403-0_3
45. Bikku, T., Gopi, A. P., & Prasanna, R. L. (2019). Swarming the high-dimensional datasets using ensemble classification algorithm. In *Advances in Intelligent Systems and Computing* (Vol. 815, pp. 583-591). https://doi.org/10.1007/978-981-13-1580-0_56
46. Sharmila, S.K., Nikhila, M., Lakshmi Prasanna, J., Lavanya, M., & Bhavana, S. (2023). Unique web-based assessment with a secure environment. *Lecture Notes in Networks and Systems, 673*, 725–736. https://doi.org/10.1007/978-981-99-1745-7_53
47. Sharmila, S.K., Lakshmi, M.S., Chowdary, G.S., Mounika, P., & Srujana, C. (2023). Speech emotion recognition using Mel Frequency Cepstral Coefficients. In *Proceedings of the 5th International Conference on Smart Systems and Inventive Technology* (ICSSIT 2023, pp. 1599–1604). https://doi.org/10.1109/ICSSIT55814.2023.10060950

48. Mohiddin, S.K., Sharmila, S., & Sharma, V. (2024). Integration of mobile edge computing in wireless technology. In *Wireless Communication Technologies: Roles, Responsibilities, and Impact of IoT, 6G, and Blockchain Practices* (pp. 1–18). https://doi.org/10.1201/9781003389231-
49. M. B. Mollah et al., "Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4157-4185, 15 March15, 2021, doi: 10.1109/JIOT.2020.3028368
50. R. C. Sofia et al., "A Framework for Cognitive, Decentralized Container Orchestration," in IEEE Access, vol. 12, pp. 79978-80008, 2024, doi: 10.1109/ACCESS.2024.3406861.